SecHack365

TrustZoneを用いた組み込みシステム

学習駆動コース　坂井ゼミ　兜森幸平

背景

- 組み込み機器によく使われているARMプロセッサにはTrustZoneというセキュリティ機能が実装されていることを知った。
- TrustZoneを用いてセキュアな組み込みシステムを開発することにした。

開発

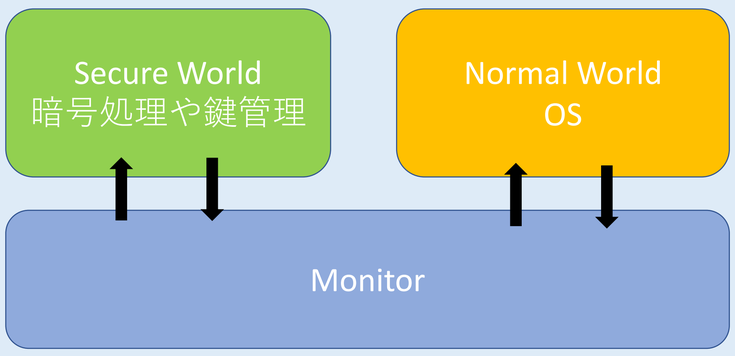
1. Normal World, Secure World, Monitor

Normal WorldとSecure Worldとそれらを切り替えるMonitorを開発している。QEMUというエミュレータ上で動作する。

流れ

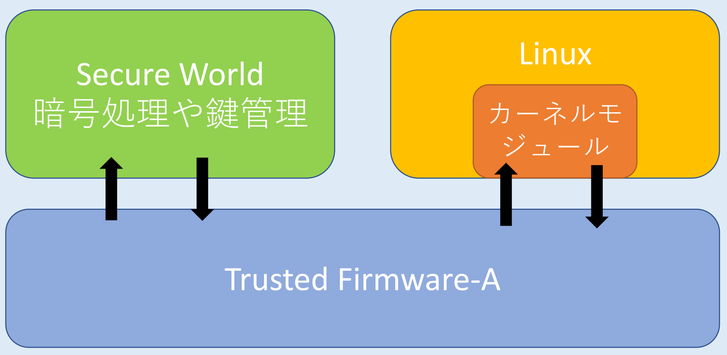
1. Monitorから実行が開始する。
2. Secure WorldとNormal Worldのバイナリをそれぞれ Secure RAMとNormal RAMにロードする。
3. Secure Worldに移行し、初期化を行う。
4. Monitorに戻り、Normal Worldに移行する。

Normal WorldではOSを、Secure Worldでは暗号処理や鍵管理を実装している。
暗号処理などをNormal WorldからSecure Worldに依頼することで機密性の高いデータを保護できる。

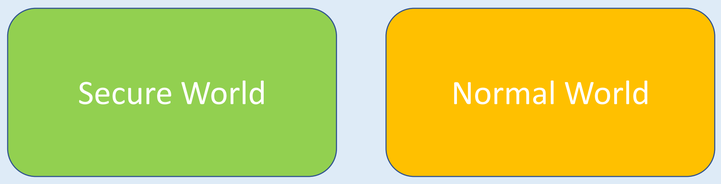


2. カーネルモジュール

Trusted Firmware-Aを用いることでNormal WorldでLinuxを動かすことができる。LinuxからSecure World側に処理を依頼するカーネルモジュールを開発している。



TrustZoneとは



- ARMプロセッサに実装されているセキュリティ機能
- CPUによってメモリをSecure WorldとNormal Worldに分割
- Normal WorldからはSecure Worldのリソースに不正にアクセスできない
- Secure Worldで機密性の高いデータを保護する

Secure World → 暗号処理、鍵管理など
Normal World → Linuxなどが動作

学習したこと

- TrustZoneの仕組み、利用方法
- TrustZoneを用いたOSであるOP-TEEの実装
- Trusted Firmware-Aの実装、仕組み、利用方法
- ARMアーキテクチャ
- 組み込みOSの実装
- カーネルモジュールの実装

今後について

開発1に関しては、Normal WorldのOS化とSecure Worldでの暗号処理や鍵管理の実装を進めていきたい。
開発2に関しては、Linuxの動作までは確認できたのでカーネルモジュールの実装を進めていきたい。
また、TrustZoneに関する資料が少ないと感じたので、今回調べたことを自分なりに資料にまとめたいと思う。

NICT 国立研究開発法人 情報通信研究機構